

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平9-107350

(43)公開日 平成9年(1997)4月22日

(51)Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
H 04 L 9/32			H 04 L 9/00	6 7 3 C
G 06 F 12/00	5 3 7		G 06 F 12/00	5 3 7 H
G 09 C 1/00	6 4 0	7259-5 J	G 09 C 1/00	6 4 0 B
H 04 L 9/10			H 04 L 9/00	6 2 1 Z
				6 2 1 A

審査請求 未請求 請求項の数 6 O L (全 13 頁) 最終頁に続く

(21)出願番号 特願平7-261241

(22)出願日 平成7年(1995)10月9日

(71)出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72)発明者 館林 誠

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 松崎 なつめ

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 原田 俊治

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(74)代理人 弁理士 滝本 智之 (外1名)

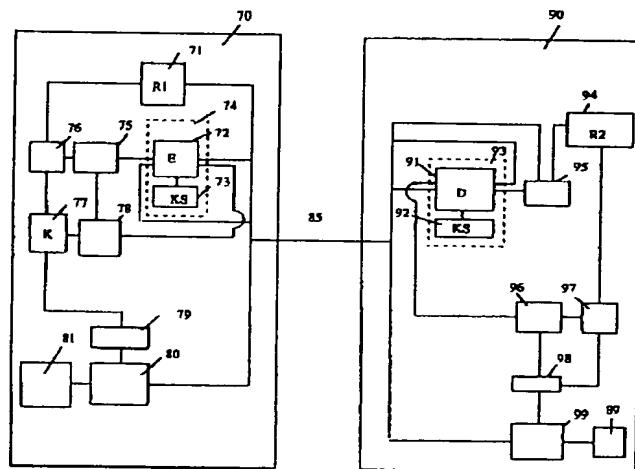
最終頁に続く

(54)【発明の名称】機器間通信保護装置

(57)【要約】

【課題】 ディジタル著作物再生装置と表示装置との間を結ぶディジタルリンクの認証と暗号化を行ってコピーを防止する。

【解決手段】 暗号アルゴリズムとして「置換」の性質をもつものを考える。このときある暗号化変換E(K₁)に対応する復号変換D(K₂)は、それ自身暗号変換となる。つまり、D(K₁, E(K₁, X))=XのときE(K₁, D(K₂, X))=Xとなる。このことにより第1の機器には暗号器Eのみ、第2の機器には復号器Dのみを備えて双方向認証することができる。その結果、(1)1つの機器には暗号器または復号器の一方だけでいいのでコンパクトになり、(2)暗号器は厳重に管理し、復号器は緩い管理にしても、復号器-復号器間の認証通信ができないので全体を厳重に管理できる。



【特許請求の範囲】

【請求項1】通信リンクにより結合される機器の間で、暗号変換およびその逆変換を用いたチャレンジ・レスポンス型の認証プロトコルにより通信相手が適切な認証鍵をもつことを確認して通信相手の正当性を認証し通信リンク上のデータの保護を行う装置であって、前記暗号変換は平文全体の集合上への置換であり、一方の機器では前記認証プロトコルにおいて暗号変換のみを行ない、他方の機器においては前記プロトコルにおいて前記暗号変換の逆変換のみを行なうことを特徴とする機器間通信保護装置。

【請求項2】通信リンクにより結合される機器の間で、暗号変換およびその逆変換を用いたチャレンジ・レスポンス型の認証プロトコルにより通信相手が適切な認証鍵をもつことを確認して通信相手の正当性を認証するとともに共通の暗号鍵を共有しこの暗号鍵を用いて暗号通信を行って通信リンク上のデータの保護を行う装置であって、前記暗号変換は平文全体の集合上への置換であり、一方の機器では前記認証プロトコルにおいて暗号変換のみを行ない、他方の機器においては前記プロトコルにおいて前記暗号変換の逆変換のみを行なうことを特徴とする機器間通信保護装置。

【請求項3】前記暗号変換および前記認証鍵からなる暗号変換モジュールと前記逆変換と前記認証鍵からなる逆変換モジュールをそれぞれモジュール外部からは前記暗号変換、前記逆変換および前記認証鍵が解析できないよう構成とし、一方のモジュールを他方とは異なる管理基準の下に提供することを特徴とする請求項1または請求項2記載の機器間通信保護装置。

【請求項4】前記暗号変換、前記逆変換、および前記認証鍵とはそれぞれ異なる第2の暗号変換とこれに対応する第2の逆変換と第2の認証鍵からなるモジュールをモジュール外部からは前記第2の暗号変換と前記第2の逆変換と前記第2の認証鍵が外部からは解析できないよう構成とし、これを通信リンクを介して通信する両方の機器に備え、これを前記認証プロトコルにおいて前記両方の機器において併用するものであり、前記変換モジュールおよび前記逆変換モジュールよりも厳しい管理基準の下に提供することを特徴とする請求項3記載の機器間通信保護装置。

【請求項5】通信リンクにより結合される機器の間で、コマンドフェーズとデータ伝送フェーズを備える機器間通信保護装置であって、前記コマンドフェーズで伝送するコマンドに認証と暗号鍵共有を起動するコマンドと、暗号通信コマンドを追加し、前記コマンドフェーズで認証と暗号鍵の共有を起動するコマンドを指定した場合に、続くデータ伝送フェーズで前記機器の間で前記通信相手の正当性を認証する処理と、その処理の結果として共通の暗号鍵の共有を行ない、次に暗号通信コマンドを指定した場合に、続く前記データ伝送フェーズで、前記

共有した暗号鍵を用いてデータを暗号変換して伝送することを特徴とする請求項2記載の機器間通信保護装置。

【請求項6】通信リンクにより結合される機器の間で、一旦リンクを分断して再度リンクを確立する機能を備える機器間通信保護装置であって、分断前に再度リンクを確立する際の通信相手の正当性認証と暗号鍵共有と暗号伝送の、すべてまたは一部に関する情報を共有する手段を有することを特徴とする請求項5記載の機器間通信保護装置。

10 【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はデジタル著作物などを処理する機器が分離しており通信リンクを介して結合されているときその通信路上のデータが不正にコピーされたり改変されたりすることを防ぐ方式と装置に関するものである。

【0002】

【従来の技術】通信路を介して通信されているデータが通信路上で不正にコピーされたり改変されることを防ぐ

20 ことが必要となる場合が数多くある。例えば、映画などの著作物がデジタル化されさらに情報圧縮され、さらに光ディスク上にデジタル記録されており、これが光ディスク再生装置により電気情報として取り出され、さらに情報伸長装置により圧縮されていたデジタル情報が伸長され、これが映像音響再生装置により再生される場合を考える。ここで光ディスク再生装置と情報伸長装置は別々の機器として分離しており、その間がデジタル通信路によりデータ通信される場合、この通信データが著作者の許可なくデジタル情報記録装置により記録

30 され、さらにデジタル情報複製装置により複製されるものであれば、その映画の著作物が不正に複製されることになり、著作権の侵害が起こる。従って通信路を介して通信されているデータが通信路上で不正にコピーされることが防がれなければならない。機器内の回路や部品の仕様が一般には公開されないのでに対し、データ通信のための電気的特性や信号形式は一般に公開される場合が多いので通信路におけるデータの不正コピーやそれに引き続くデータの改変が大きな問題になる。

【0003】このような機器間通信保護装置の構成法について従来より様々なものが知られている。最も代表的なものは相手認証技術を用いるものである。これは基本的にはデータを送出する側が受信する側の正当性を認証し、正当な受信者であることが確認できたときのみにデータを送信することによりデータが不正な機器に受信されることがないようにするものである。この場合の受信者のように自らの正当性を証明する側を証明者と呼び、またこの場合の送信者のように相手の正当性を確認する側を認証者と呼ぶ。

【0004】前述の光ディスク記録再生に関わる機器のような場合、特定の機器の間で認証が行われるというよ

りも、光ディスク関連機器の業界によって定まる規格に従って作成されたかどうかが問題となる。従ってこの場合、「正当性」とは「所定の規格に準拠すること」を意味する。

【0005】従来の技術の一例として国際標準規格 ISO/IEC 9798-2に記載される暗号技術を用いた一方向認証方法がある。この認証方法は証明者が認証鍵と呼ばれる秘密のデータを持つことを、その鍵自身を知らせることなく証明者に対して証明することを基本としている。するためにまず認証者があるデータを選びこれを証明者に対して投げかける。これをチャレンジを呼ぶ。これに対し証明者がある暗号変換を保有し前記認証鍵を用いて前記チャレンジデータを暗号化する。このように暗号化されたデータをレスポンスとして認証者に対して返す。このレスポンスを受信した認証者は前記暗号変換の逆変換である復号変換と認証鍵を共有しており、このレスポンスを前記認証鍵を用いて前記復号変換によって復号する。この結果が前記チャレンジと一致すれば受信者は正規の認証鍵を持つものと判断し、証明者の正当性を認証する。一方向認証とは一方の側がその正当性を他方に証明することを意味している。

【0006】暗号変換Tとは、鍵情報Kにより定まる平文集合から暗号文集合への写像である。平文をXとしたとき暗号文を $T(K, X)$ と書く。同じ鍵情報Kにより定まる暗号文集合から平文集合への写像である逆変換 T^{-1} との間には、

$$T^{-1}(K, T(K, X)) = X$$

の関係がある。これは平文Xを暗号変換し、これを逆変換すると元に戻ることを意味している。暗号の場合、暗号変換の逆変換を特に復号変換と呼ぶ。暗号変換であるためには鍵Kの知識がないときに $T(K, X)$ からXを求めることが必要である。以降では慣例により暗号変換を $E(K, \cdot)$ 、復号変換を $D(K, \cdot)$ と記す。

【0007】図6は前記規格に記載されている認証方法を実現する装置の一例である。図6において、10は第1の機器、11は乱数発生部、12はある暗号アルゴリズムの復号器、13は第2の機器の認証鍵K2を格納する第1の認証鍵格納部、14はデータ比較部、15は著作物送信ゲート、16は著作物データ格納部である。11から16は第1の機器10の構成要素である。20は通信路である。30は第2の機器、32は前記暗号アルゴリズムの暗号器、33は第2の機器の認証鍵K2を格納する第2の認証鍵格納部、34は著作物データ処理部である。32から34は第2の機器30の構成要素である。

【0008】この従来の一方向認証方法の動作を図7の動作説明図に従い説明する。

(1) 第1の機器10が通信路20を介して第2の機器30に対して著作物データ格納部16に格納されている著作物データを送信しようとする場合、まず第1の機器10は乱数発生部11において乱数Rを生成する。そし

てこれをチャレンジデータCHAとして通信路20に対して送出する。

$$【0009】 CHA = R$$

(2) 第2の機器30はこの乱数を受けとると、この乱数を平文とし、第2の認証鍵格納部33に格納されている認証鍵K2を暗号鍵として暗号器32により暗号化する。そしてその結果RESをレスポンスとして通信路に対して送出する。

$$【0010】 RES = E(K2, CHA)$$

10 (3) この電文RESを受けとった第1の機器10はこのレスポンスデータRESを暗号文とし、第2の機器の認証鍵格納部13に格納されている認証鍵K2を復号鍵として復号部12において復号する。

$$【0011】 D(K2, RES) = RR$$

そしてこの結果をデータ比較部14において乱数発生部11に一時保管されている乱数Rと比較する。これが一致すれば通信相手は第2の機器30の認証鍵を保有するものと考え、通信相手が正当なものであると認証して

20 (4) に進む。一方一致しなければ通信相手が正当なものではないものと判断して処理を中断する。

(4) このように第1の機器10が第2の機器30を正当なものとみなせば、第1の機器は著作物データ格納部16に格納されている著作物データを通信路20を介して第2の機器30に伝達する。これを受信した第2の機器30はこの著作物データを著作物データ処理部34において処理される。

【0012】もしも、第2の機器の代わりに第2の機器の認証鍵を有さない第3の機器が通信路20に接続されている場合、その第3の機器は上記ステップ(2)で正しい値のデータを作成することができない。従って第1の機器は上記ステップ(3)で通信相手が正しくない機器であるものと判断する。このようにして著作権のあるデータは不正な機器に伝送されることがない。

【0013】なお、第1の機器と第2の機器の間でいつも同じチャレンジとレスポンスデータが用いられるならばこれを用いて不正な第3の機器が第2の機器になりますことが考えられる。これを避けるために第1の機器からは毎回異なるチャレンジを送る。

40 【0014】しかしながら、上記に示したように第1の機器が正規の認証鍵を持つ第2の機器を認証した後著作権データを通信路20を介して第2の機器に伝送している最中に、この通信路上のデータを抜きとり、これを例えればハードディスク装置に記憶することが考えられる。もちろんこのためには通信路上の信号の電気的特性やデータ形式などの知識が必要であるがこれは特に秘密にされている情報ではないのでデジタルデータの抜きとりは技術的に十分に可能である。同様にしてこのようにハードディスク装置に記憶されているデータを正規の認証鍵を有する第2の機器に対して送出することも可能である。従って、上記の一方向認証方法だけでは著作権デー

タの保護は不完全である。この課題を解決するために、第1の機器が第2の機器の正当性を確認すると同時に第2の機器が第1の機器の正当性を確認することが必要となる。

【0015】このように上記の一方向認証を組み合わせて双方向認証を行なう方法も上記国際標準規格に述べられている。

【0016】図8はこの双方向認証方式を実現する装置の一例を示すものである。但し、ここでは双方向認証方式を実現するのみならず、双方向認証の処理の結果、2つの機器にランダムな鍵が共有されるようになっている。この共有鍵はこの認証プロトコルに引き継ぎ行なわれる暗号通信のための暗号／復号鍵に用いられるものである。

【0017】図8において、40は第1の機器、41は第1の乱数発生部、42は第1の暗号アルゴリズムの復号器、43は第2の機器の認証鍵K2を格納する第1の認証鍵格納部、44は第1のデータ分離部、45は第1のデータ比較部、46は第3の乱数発生部、47は第2の暗号アルゴリズムの暗号器、48は第1の機器の認証鍵K1を格納する第2の認証鍵格納部である。49は第1の共有鍵一時格納部、50はデータ暗号器、51は著作物データ格納部、52は第1のデータ連結部である。41から52は第1の機器40の構成要素である。55は通信路である。60は第2の機器、61は前記第1のアルゴリズム復号器42に対応する第1の暗号アルゴリズムの暗号器、62は第2の機器の認証鍵K2を格納する第3の認証鍵格納部、63は第2の乱数発生部、64は前記第2の暗号アルゴリズムの復号器、65は第1の機器の認証鍵K1を格納する第4の認証鍵格納部、66は第2のデータ分離部、67は第2のデータ比較部、68は第2の共有鍵一時格納部、69はデータ復号器、58は第2のデータ連結部、59は著作物データ処理部である。61から69、58、59は第2の機器60の構成要素である。

【0018】この従来の双方向認証方法の動作を図9の動作説明図に従い説明する。

(1) まず、第1の機器40は第1の乱数発生部41において乱数R1を生成する。これは第1のチャレンジCHA1としての意味を持つ。そしてこれを通信路55に対して送出する。

(2) 第2の機器60はこの乱数R1を受けると、第2の乱数発生器63において第2の乱数R2を発生し、第2のデータ連結部58において第1の乱数R1と第2の乱数R2の連結R1||R2を作成する。そしてこれを平文とし、第3の認証鍵格納部62に格納されている第2の機器の認証鍵K2を暗号鍵として第1の暗号アルゴリズムの暗号器61により暗号化する。

【0019】RESCHA = E(K2, R1||R2)

ここでR2は第2のチャレンジとしての意味を持つ。暗号 50

化した結果は第1のチャレンジに対するレスポンスおよび第2のチャレンジの両方の意味を持つ。そしてその結果RESCHAを通信路55に対して送出する。

(3) この電文RESCHAを受けとった第1の機器40はこれを暗号文とし、第1の認証鍵格納部43に格納されている第2の機器の認証鍵K2を復号鍵として第1の復号部42において復号する。

【0020】D(K2, RESCHA) = X1

そしてその結果X1を第1のデータ分離部44に入力する。第1のデータ分離部44は入力されたデータを第1の乱数部分RR1と第2の乱数部分のデータRR2に分離する。

【0021】X1 : RR1 || RR2

そして第1の乱数部分のデータRR1を第1のデータ比較部45に対して送出する。第1のデータ比較部45はこのデータRR1を第1の乱数発生部41に一時記憶されている乱数R1と比較する。これが一致すれば通信相手が第2の機器60の認証鍵K2を持っていることを証明したものと考え、通信相手が間違いなく第2の機器60であるものと認証し(4)に進む。もしも一致しなければここで認証処理を中断する。

(4) 第3の乱数発生部46は第3の乱数Kを発生する。そして第1のデータ連結部52は第1のデータ分離部44において分離された第2の乱数部分のデータRR2とこの乱数Kを連結しその結果RR2||Kを第2の暗号アルゴリズムの暗号器47に渡す。暗号器47はこれを平文とし、第2の認証鍵格納部48に格納されている第1の機器の認証鍵K1を暗号鍵として暗号化する。

【0022】RES2 = E(K1, RR2||K)

30 その結果RES2を通信路55に対して送出する。

(5) この電文を受けとった第2の機器60はこのレスポンスデータRES2を暗号文とし、第4の認証鍵格納部65に格納されている第1の機器の認証鍵K1を復号鍵として第2の暗号アルゴリズムの復号部64において復号する。

【0023】D(K1, RES2) = X2

そしてその結果X2を第2のデータ分離部66に入力する。第2のデータ分離部66は入力されたデータを第2の乱数部分RRR2と第3の乱数部分KKのデータに分離する。

【0024】X2 : RRR2 || KK

そして第2の乱数部分のデータRRR2を第2の比較部67に対して送出する。第2の比較部67はこのデータRRR2を第2の乱数発生部63に一時記憶されている乱数R2と比較する。これが一致すれば通信相手は第1の機器40の認証鍵K1を持っていることを証明したものと考え、通信相手が間違いなく第1の機器40であることを認証する。そして(6)に進む。もしも一致しなければ認証は失敗したものとして認証処理を終る。

(6) 第2のデータ分離部で分離された第3の乱数KK

(これはKに等しいことが確認されている)を第2の共有鍵一時格納部68に設定する。そして第1の機器40に対して認証した旨の信号を送る。

(7) 第2の機器60から認証した旨の信号を受けた第1の機器40は第3の乱数発生部46で生成した乱数Kを第1の共有鍵一時格納部49に転送する。そしてデータ暗号器50は著作物データ格納部51から入力される著作物データをこの乱数Kを暗号鍵として用いて暗号化しその結果を通信路55に対して送出する。

(8) この電文を受け取った第2の機器60はデータ復号器69に入力されるデータを第2の共有鍵一時格納部68に格納されているデータを復号鍵として復号しこれを著作物データ処理部59に対して出力する。

【0025】第1の機器40と第2の機器60がどちらも正当なものであれば共有鍵一時格納部68に格納されているデータは前記第1の共通鍵一時格納部に格納されているデータと等しくなるので(7)のステップで暗号化されたデータが正しく復号される。

【0026】もしも第1の機器が正規の認証鍵を有し、第2の機器が正規の認証鍵を有していない場合、ステップ(3)で第1の機器は通信相手が正規の認証鍵を有していないものと判断し、認証処理を中断できる。また第1の機器が正規の認証鍵を有しておらず、第2の機器は正規の認証鍵を有している場合、ステップ(5)において第2の機器は通信相手が正規の認証鍵を有していないものと判断し、認証処理を中断する。このようにして著作権データが不正な機器に流出することとともに不正な機器から正規の機器に流入することが防止できる。

【0027】また、第1の機器も第2の機器も正当な認証鍵を有している場合で、認証処理が完了し、ステップ(7) (8)において著作権データが通信路上を伝送されているものを電気的にコピーしてデジタル蓄積装置に蓄積したとしてもそのデジタルデータは暗号化されており、無意味なものなので著作権データを有效地に保護できる。

【0028】以上の説明においては第1の機器による第2の機器の認証には第1の暗号アルゴリズムを用い、第2の機器による第1の機器の認証には第2の暗号アルゴリズムを用いるものとした。このように別の暗号アルゴリズムを用いるのではなくそれぞれに同じ暗号アルゴリズムを用いてよい。この場合、第1の暗号アルゴリズムの復号器42と第2の暗号アルゴリズムの復号器64とは同一のものとなる。以下ではこれを復号器と呼ぶ。同様に第1の暗号アルゴリズムの暗号器61と第2の暗号アルゴリズムの暗号器47は同一のものとなる。以下ではこれを暗号器と呼ぶ。

【0029】以上のように暗号アルゴリズムを用いた双方認証が首尾よく行われるには、第1の機器および第2の機器の内部に格納されている認証鍵が不正を行おうとするものに容易に分からぬことが前提となる。この

ために最も効果的な方法は、上記の暗号器と第1のまたは第2の機器の認証鍵の一対を同じ集積回路の中につじ込めて実現するものである。こうすれば、その集積回路の解析には多大な労力がかかるので認証鍵が容易には分からぬこととなる。同様に復号器と第1または第2の機器の認証鍵の一対を同じ集積回路の中につじ込める。

【0030】上記の例では第1の機器では復号器と第2の機器の認証鍵の対、暗号器と第1の機器の認証鍵の対が必要となり、第2の機器では暗号器と第2の認証鍵の対、復号器と第1の機器の認証鍵の対が必要となる。また、機器の認証鍵についても第1の機器と第2の機器の違いは重要ではなく、ある特定の基準を満たす機器であることを他と区別する必要だけがある場合であったとしても、第1の機器にも第2の機器にも暗号器と認証鍵の対、および復号器と認証鍵の対が各1対必要となる。

【0031】このように従来の機器間相互認証方式において特定の規格を満たす機器であることを相互に認証を行なう場合、各機器ごとに暗号器と認証鍵の対、および復号器と認証鍵の対、の2つの集積回路が必要となり機器のコストアップにつながるという問題点を有するものであった。

【0032】上述のように特定規格を満たす機器であることを機器同士が確認して著作権データが規格外の機器に流出することを防止するためには、暗号器と認証鍵の対、および復号器と認証鍵の対の集積回路を設けることが効果的である。この場合、これらの集積回路はある管理の下で機器製造者に配布されなければならない。その管理とは正規の機器の製造にのみこれらの集積回路が利用されることを目的とした管理である。ところが、複数の機器製造者が存在する場合このような管理を完全に実施することは難しい。必ず、これらの集積回路を用いて不正な機器が製造される可能性がある。以下ではこの場合どのようなことが起るかを考察する。

【0033】暗号器・認証鍵対、および復号器・認証鍵対の各1対があれば正規の機器から著作権データを吸い上げる機器が実現できることは明らかである。ある不正な機器製造者がこのようにして不正なデジタル情報記録再生装置を作成したものとする。この装置は情報記録装置として動作するときには正規の機器から著作権データを吸い上げる。そして情報再生装置として動作するときには正規の機器に対して著作権データを吐き出す。このようにして著作権データの不正なコピーが可能となる。このことは、暗号器・認証鍵対と復号器・認証鍵対の両方を持つことに起因しているのである。

【0034】このように、従来の機器間通信保護装置を実現しようとすると、不正な情報機器の製造を制限することが困難であるという問題点を有するものであった。

【0035】また、従来の機器間通信のためには、通信リンクにより結合される機器の間でコマンドフェーズとデータ伝送フェーズを備えたものはあったが、前述のよ

うなコンパクトさと安全性を備えた特徴を持つものは存在しなかった。

【0036】

【課題を解決するための手段】本発明は従来の機器間通信保護装置にあった上記のような欠点を改善するためになされたものであり、請求項1に係る発明は、通信リンクにより結合される機器の間で、暗号変換およびその逆変換を用いたチャレンジ・レスポンス型の認証プロトコルにより通信相手が適切な認証鍵をもつことを確認して通信相手の正当性を認証し通信リンク上のデータの保護を行う装置であって、前記暗号変換は平文全体の集合上への置換とし、一方の機器では前記認証プロトコルにおいて暗号変換であるのみを行ない、他方の機器においては前記プロトコルにおいて前記暗号変換の逆変換のみを行なう手段を有している。

【0037】請求項2に係る発明は、通信リンクにより結合される機器の間で、暗号変換およびその逆変換を用いたチャレンジ・レスポンス型の認証プロトコルにより通信相手が適切な認証鍵をもつことを確認して通信相手の正当性を認証するとともに共通の暗号鍵を共有しこの暗号鍵を用いて暗号通信を行って通信リンク上のデータの保護を行う装置であって、前記暗号変換は平文全体の集合上への置換であり、一方の機器では前記認証プロトコルにおいて暗号変換のみを行ない、他方の機器においては前記プロトコルにおいて前記暗号変換の逆変換のみを行なう手段を有している。

【0038】請求項3に係る発明は、請求項1および2の発明において、前記暗号変換および前記認証鍵からなる暗号変換モジュールと前記逆変換と前記認証鍵からなる逆変換モジュールをそれぞれモジュール外部からは前記暗号変換、前記逆変換および前記認証鍵が解析できないような構成とし、一方のモジュールを他方とは異なる管理基準の下に提供することを特徴としている。

【0039】請求項4に係る発明は、請求項3の発明において、前記暗号変換、前記逆変換、および前記認証鍵とはそれぞれ異なる第2の暗号変換とこれに対応する第2の逆変換と第2の認証鍵からなるモジュールをモジュール外部からは前記第2の暗号変換と前記第2の逆変換と前記第2の認証鍵が外部からは解析できないような構成とし、これを通信リンクを介して通信する両方の機器に備え、これを前記認証プロトコルにおいて前記両方の機器において併用するものであり、前記変換モジュールおよび前記逆変換モジュールよりも厳しい管理基準の下に提供することを特徴としている。

【0040】請求項5に関わる発明は、請求項2の発明において、通信リンクにより結合される機器の間で、コマンドフェーズとデータ伝送フェーズを備えており、前記コマンドフェーズで伝送するコマンドに認証と暗号鍵共有を起動するコマンドと、暗号通信コマンドを追加し、前記コマンドフェーズで認証と暗号鍵の共有を起動

するコマンドを指定した場合に、続くデータ伝送フェーズで前記機器の間で通信相手の正当性を認証する処理と、その処理の結果として共通の暗号鍵の共有を行ない、次に暗号通信コマンドを指定した場合に、続く前記データ伝送フェーズで、前記共有した暗号鍵を用いてデータを暗号変換して伝送する構成としている。

【0041】請求項6の発明は、請求項5の発明において、一旦リンクを分断して再度リンクを確立する機能を備え、分断前に再度リンクを確立する際の通信相手の正当性認証と暗号鍵共有と暗号伝送の、すべてまたは一部に関する情報を共有する手段を有している。

【0042】

【発明の実施の形態】請求項1の発明は前記の構成をとることにより、認証プロトコルを実現するとき、一方の機器では暗号変換のみを行ない、他方の機器においては前記暗号変換の逆変換のみを行なうことが可能となり、暗号変換とその逆変換の両方を有する必要がなくコンパクトに実現できるようになった。

【0043】請求項2の発明は前記の構成をとることにより、認証および鍵共有プロトコルを実現するとき、一方の機器では暗号変換のみを行ない、他方の機器においては前記暗号変換の逆変換のみを行なうことが可能となり、暗号変換とその逆変換の両方を有する必要がなくコンパクトに実現できるようになった。

【0044】請求項3の発明は前記の構成をとることにより、暗号変換モジュールと暗号モジュール間、復号モジュールと復号モジュール間では認証ができないため、暗号モジュールまたは復号モジュールの一方の提供を厳重に管理することにより、装置間通信保護の効力を高めることができる。

【0045】請求項4の発明は前記の構成をとることにより、前記暗号モジュールおよび復号モジュールとは異なる別のモジュールをより厳密な管理状態で提供することにより、装置間通信保護の効力を高めることができる。

【0046】請求項5および6の発明は前記の構成をとることにより、機器間通信装置に正当性認証と暗号鍵共有と暗号伝送の保護機能のすべてまたはその一部の機能を追加することができる。

【0047】(実施例1) 図1は本発明の機器間通信保護装置の第1の実施例を示すブロック図である。

【0048】図1において、70は第1の機器、71は第1の乱数発生部、72は下記の条件を満たす暗号変換の暗号器、73は機器認証鍵を格納する第1の認証鍵格納部であり、72と73は暗号モジュール74として集積回路の形で一体化されている。75は第1のデータ分離部、76は第1のデータ比較部、77は第3の乱数発生部、78は第1のデータ連結部、79は第1の共有鍵一時格納部、80はデータ暗号器、81は著作物データ格納部である。71から81は第1の機器の構成要素で

ある。85は通信路である。90は第2の機器、91は前記暗号変換の復号器、92は機器認証鍵を格納する第2の認証鍵格納部であり、91と92は復号実現モジュール93として集積回路の形で一体化されている。94は第2の乱数発生部、95は第2のデータ連結部、96は第2のデータ分離部、97は第2のデータ比較部、98は第2の共有鍵一時格納部、99はデータ復号器、89は著作物処理部である。91から99、89は第2の機器の構成要素である。

【0049】ここで前記暗号変換の満たすべき条件を述べる。暗号変換をE、Eに対する逆変換（復号変換）をDとする。このとき、Eは平文全体の集合S1から暗号文全体の集合S2への写像、そしてDはS2からS1への写像と考えられる。この時、EがS1上の置換であることが満たすべき条件である。

【0050】写像Eが置換であるとは、以下の条件を満たすときにいう：

(1) $S1 = S2$ 、(2) Eが単射である、(3) Eが全射である。

【0051】ここでEが単射であるとは、「 $S1$ の元 x 、 y に対して、 $E(x) = E(y)$ である場合は、 $x = y$ の場合に限る」ことをいう。またEが全射であるとは、「任意の $S2$ の元 z に対して、ある $S1$ の元 w が存在して、 $E(w) = z$ を満たす」ことをいう。このとき、Eの復号アルゴリズムDも $S1$ 上の置換となる。

【0052】次にEが $S1$ 上の置換である場合に満たすべき性質について述べる。まず全射Eが暗号アルゴリズムで、DがEに対する復号アルゴリズムであることから、任意の $S1$ の元 x 、すなわち平文 x 、に対して、暗号文 $E(x)$ がEの復号アルゴリズムDで平文 x に復号されるのであるから、

$$D(E(x)) = x \quad \text{--- (*1)}$$

が成り立つ。ここで、 $S1 = S2$ であるから任意の $S1$ の元 x 、すなわち平文 x 、に対して、D(x)は $S1$ の元となるから、上記(*1)式の x としてD(x)を取ると、

$$D(E(D(x))) = D(x) \quad \text{--- (*2)}$$

が成り立つ。今、E、Dが $S1$ 上の置換であるから、Dは単射である。よって式(*2)から、

$$E(D(x)) = x \quad \text{--- (*3)}$$

が成り立つ。すなわち、ある平文 x に対してDという

(復号)変換を行った結果に対してEという逆変換を行った結果は元に平文に戻る。このように、変換Dが一種の暗号変換になることが重要なポイントである。

【0053】この実施例の機器間通信保護装置の動作を図2の動作説明図に従い説明する。本実施例は請求項2に対応するものである。

(1) まず、第1の機器70は第1の乱数発生部71において乱数R1を生成する。これは第1のチャレンジCHA1としての意味を持つ。そしてこれを通信路85に対して

送出する。

(2) 第2の機器90はこの電文CHA1（その内容は乱数R1である）を受けとると、第2の乱数発生器94において第2の乱数R2を発生し、第2のデータ連結部95において第1の乱数R1と第2の乱数R2を連結しこれを平文とし、第2の認証鍵格納部92に格納されている機器認証鍵KSを復号鍵として復号器91により復号変換する。

$$【0054】 RESCHA = D(KS, R1 || R2)$$

ここで平文を復号変換するとは一種の暗号化を行うことを意味しており、その出力は乱数のように見える。ここでR2は第2のチャレンジとしての意味を持つ。復号化した結果は第1のチャレンジに対するレスポンスと第2のチャレンジの両方の意味を持つ。そしてその結果を通信路85に対して送出する。

(3) この電文RESCHAを受けとった第1の機器70はこのレスポンスデータを暗号文とし、第1の認証鍵格納部73に格納されている機器認証鍵KSを暗号鍵として暗号器72において暗号変換する。

$$【0055】 X1 = E(KS, RESCHA)$$

この場合の暗号変換とは前記復号変換の逆変換、すなわち復号化することに他ならない。そしてその結果X1を第1のデータ分離部75に入力する。第1のデータ分離部75は入力されたデータを第1の乱数部分RR1と第2の乱数部分RR2のデータに分離する。

$$【0056】 X1 : RR1 || RR2$$

そして第1の乱数部分のデータRR1を第1のデータ比較部76に対して送出する。第1のデータ比較部76はこのデータRR1を第1の乱数発生部71に一時記憶されている乱数R1と比較する。これが一致すれば通信相手が正規の機器認証鍵KSを持っていることを証明したものと考え、通信相手が間違いなく正規機器であるものと認証し(4)に進む。もしも一致しなければここで認証処理を中断する。

(4) 第3の乱数発生部77は第3の乱数Kを発生する。第1のデータ連結部78は第1のデータ分離部75において分離された第2の乱数部分のデータRR2とこの乱数Kを連結し、これを暗号器72に送り、暗号器72はこの連結されたデータを平文とし、第1の認証鍵格納部73に格納されている機器認証鍵KSを暗号鍵として暗号変換する。

$$【0057】 RES2 = E(KS, RR2 || K)$$

そしてこの結果（第2のレスポンス）を通信路55に対して送出する。

(5) この電文RES2を受けとった第2の機器60はこのレスポンスデータを暗号文とし、第2の認証鍵格納部92に格納されている機器認証鍵KSを復号鍵として前記暗号アルゴリズムの復号部92において復号する。

$$【0058】 X2 = D(KS, RES2)$$

そしてその結果X2を第2のデータ分離部96に入力する。第2のデータ分離部96は入力されたデータX2を第

2の乱数部分のデータRRR2と第3の乱数部分のデータKKに分離する。

【0059】 X2 : RRR2 || KK

そして第2の乱数部分のデータRRR2を第2のデータ比較部97に対して送出する。第2のデータ比較部97はこのデータRRR2を第2の乱数発生部93に一時記憶している乱数R2と比較する。これが一致すれば通信相手は正規の機器認証鍵を持っていることを証明したものと考え、通信相手が間違いなく正規の機器であることを認証する。そして(6)に進む。もしも一致しなければ認証は失敗したものとして認証処理を終る。

(6) 第2のデータ分離部96で分離された第3の乱数KK(これが乱数Kに等しいことは確認されている)を第2の共有鍵一時格納部98に設定する。そして第1の機器70に対して認証した旨の信号を送る。

(7) 第2の機器90から認証した旨の信号を受けた第1の機器70は第3の乱数発生部77で生成した乱数Kを第1の共有鍵一時格納部79に転送する。そしてデータ暗号器80は著作物データ格納部81に格納されているデータをこの乱数Kを暗号鍵として用いて暗号化しその結果を通信路85に対して送出する。

(8) この電文を受け取った第2の機器90はデータ復号器99に入力されるデータを第2の共有鍵一時格納部98に格納されているデータを復号鍵として復号する。そしてこの結果を著作物処理部89において処理する。

【0060】第1の機器70と第2の機器90がどちらも正当なものであれば共有鍵一時格納部68に格納されているデータは前記第1の共通鍵一時格納部に格納されているデータと等しくなるので(8)のステップで暗号化されたデータが正しく復号される。

【0061】もしも第1の機器が正規の認証鍵を有し、第2の機器が正規の認証鍵を有していない場合、ステップ(3)で第1の機器は通信相手が正規の認証鍵を有していないものと判断し、認証処理が中断される。また第1の機器が正規の認証鍵を有しておらず、第2の機器は正規の認証鍵を有している場合、ステップ(5)において第2の機器は通信相手が正規の認証鍵を有していないものと判断し、認証処理を中断する。従って、第2の共有鍵一時格納部には正しい共有鍵が設定されない。このようにして著作権データが不正な機器に流出することとともに不正な機器から正規の機器に流入することが防止できる。

【0062】また、第1の機器も第2の機器も正当な認証鍵を有している場合で、認証処理が完了し、ステップ(7) (8)において著作権データが通信路上を伝送されているものを電気的にコピーしてディジタル蓄積装置に蓄積したとしてもそのディジタルデータは暗号化されており、無意味なものなので著作権データを有効に保護できる。

【0063】本実施例では第1の機器では暗号器と認証

10

鍵の対、第2の機器では復号器と認証鍵の対、だけが必要となる。これは従来の機器間通信保護装置が第1の機器にも第2の機器にも暗号器と認証鍵の対、および復号器と認証鍵の対が各1対必要となることと比較すると集積回路が1つでよく機器のコストダウンにつながるという効果がある。

【0064】さらに、暗号器と認証鍵の対となる集積回路、および復号器と認証鍵の対となる集積回路はある管理の下で機器製造者に配布されなければならない。その管理とは正規の機器の製造にのみこれらの集積回路が利用されることを目的とした管理である。ところが、複数の機器製造者が存在する場合このような管理を完全に実施することは難しい。必ず、これらの集積回路を用いて不正な機器が製造される可能性がある。以下ではこの場合どのようなことが起こるかを考察する。

【0065】暗号器・認証鍵対の集積回路は厳重な管理の下で機器製造者に提供されるものとしよう。一方復号器・認証鍵対の集積回路は前記管理ほど厳重ではない形で機器製造者に提供されるものとしよう。このとき暗号器・認証鍵対の集積回路は光ディスクなどに格納されている著作権データを受け取りこれを通信リンクを介して提供する側の機器(これを提供側機器とよぶ)に設置するものとし、復号器・認証鍵対の集積回路は前記機器から通信リンクを介して著作権データの提供を受ける側の機器(これを獲得側機器とよぶ)に設置するものと決めておく。前述のように暗号器・認証鍵対の集積回路は厳重な管理の下で提供側機器製造者に提供されるので正規の提供側機器しか作成できない。一方復号器・認証鍵対の集積回路は前記管理ほど厳重ではない形で機器製造者

20

に提供されるため、ある不正な機器製造者が本来の契約に反して獲得側および提供側の両方の性質をもった機器を作成する可能性がある。例えば不正なディジタル情報記録再生装置を作成しようとしたものとする。この装置は情報記録装置として動作するときには正規の提供側機器から著作権データを獲得する機器である。復号器・認証鍵対の集積回路があるから前記の双方向認証が可能となり正規の提供側機器から著作権データを獲得することができる。一方、情報再生装置として動作するときには正規の獲得側機器に対して著作権データを提供することが必要である。ところが著作権データの獲得側機器には復号器・認証鍵対しか備えられていないため著作権データの提供のためには暗号器・認証鍵対の集積回路が必要となる。前述のように厳密な管理によりこのような集積回路が入手できないので結局このような不正な機器を作成することができない。以上の説明は請求項3に関わる。

30

【0066】なお、本実施例においては双方の認証の後に鍵共有を行うものとしたが暗号通信の必要のない場合にはこの部分は割愛することができる。これは請求項1に関わる。

40

【0067】本実施例では第1の機器では暗号器と認証

50

【0067】また、本実施例においては、チャレンジは平文、レスポンスは暗号文（復号文）という場合であり、さらに第2の機器から第1の機器への第1のレスポンスと第2のチャレンジを合成したプロトコルを説明したが、本発明の認証プロトコルはこの方法に限定されるものではなく、チャレンジは乱数を暗号化（復号化）したもの、レスポンスはこれを復号化（暗号化）したものというようにすることも可能である。本発明のポイントは認証プロトコルの如何によらず一方の機器には暗号化モジュールまたは復号化モジュールのいづれか一方しかないことによりコストダウンを図りさらにこのモジュールの不正使用に対する安全性を増したところにある。

【0068】（実施例2）図3は本発明の機器間通信保護装置の第2の実施例を示すブロック図である。同図を図1と比べると第1の機器70においては第2の暗号アルゴリズムの暗号器82および第2の機器認証鍵KS2を格納する第5の認証鍵格納部83が追加されている。この2つの構成要素は第2の暗号モジュール84として集積回路などの形で一体化されている。第2の機器90においては第2の暗号アルゴリズムの暗号器101および第2の機器認証鍵KS2を格納する第6の認証鍵格納部102が追加されている。この2つは第3の暗号モジュール103として集積回路などの形で一体化されている。これ以外は図1の対応する番号の構成要素と同じである。

【0069】ここで第2の暗号アルゴリズムは第1の実施例で述べた置換の性質を備える必要はなく、一般的の暗号アルゴリズム（本明細書の従来技術で述べたもの）でよい。ただし後述のようにこの場合はこの暗号モジュールが不正利用されないように厳重に管理されなければならない。

【0070】第2の実施例の機器間通信保護装置の動作を図4の動作説明図に従い説明する。本実施例は請求項4に対応するものである。

（1）まず、第1の機器70は第1の乱数発生部71において乱数R1を生成する。これは第1のチャレンジCHAIとしての意味を持つ。そしてこの電文CHAIを通信路85に対して送出する。

（2）第2の機器90はこの電文CHAI（その内容は乱数R1）を受けとると、これを第2の暗号アルゴリズムの暗号器101の入力とする。第2の暗号アルゴリズムの暗号器101は第6の認証鍵格納部に格納されている第2の機器認証鍵KS2を鍵として暗号化を行って暗号文データを作成する。

【0071】 $X1 = e(KS2, R1)$

一方第2の乱数発生器94において第2の乱数R2を発生し、第2のデータ連結部95において前記暗号文データX1と第2の乱数R2を連結し、これを平文として、第2の認証鍵格納部92に格納されている機器認証鍵KSを復号鍵として暗号アルゴリズムの復号部92において復号する。

する。

【0072】 $RESCHA = D(KS, X1 || R2)$

ここで平文を復号変換するとは一種の暗号化を行っていることに他ならず、その出力は乱数のように見える。ここでR2は第2のチャレンジとしての意味を持つ。復号変換した結果は第1のチャレンジに対するレスポンスおよび第2のチャレンジの両方の意味を持つ。そしてその結果RESCHAを通信路85に対して送出する。

（3）この電文RESCHAを受けとった第1の機器70はこのデータを暗号文とし、第1の認証鍵格納部73に格納されている認証鍵KSを暗号鍵として暗号器72において暗号変換する。この場合の暗号変換とは平文に戻すことである。

【0073】 $X2 = E(KS, RESCHA)$

そしてその結果X2を第1のデータ分離部75に入力する。第1のデータ分離部75は入力されたデータX2を前記暗号文データ部分XX1と第2の乱数部分のデータRR2に分離する。そして前記暗号文データ部分のデータXX1を第1のデータ比較部76に対して送出する。一方第1の乱数発生部71に一時記憶されている乱数R1は第2の暗号アルゴリズムの暗号器82に送られここで第5の認証鍵格納部83に格納されている第2の機器認証鍵KS2を暗号鍵として暗号化される。

【0074】 $X3 = e(KS2, R1)$

その結果X3は第1のデータ比較部76において前記暗号文データ部分のデータXX1と比較される。これが一致すれば通信相手が第2の機器90の認証鍵および第2の認証鍵を持っていることを証明したものと考え、通信相手が間違いなく正規の機器であるものと認証し（4）に進む。もしも一致しなければここで認証処理を中断する。

（4）第2の暗号アルゴリズムの暗号器82は第1のデータ分離部75において分離された第2の乱数部分のデータRR2を入力とし第5の認証鍵格納部83に格納されている第2の機器認証鍵KS2を鍵として暗号化を行って暗号文データを作成する。

【0075】 $X4 = e(KS2, RR2)$

一方第3の乱数発生部77は第3の乱数Kを発生する。そして暗号アルゴリズムの暗号器72は前記データX4この乱数Kを第1のデータ連結部78において連結したものを平文とし、第1の認証鍵格納部73に格納されている機器認証鍵を暗号鍵として暗号化する。

【0076】 $RES2 = E(KS, X4 || K)$

そしてこの結果を第2のレスポンスRES2としてを通信路55に対して送出する。

（5）この電文を受けとった第2の機器60はこのレスポンスデータを暗号文とし、第2の認証鍵格納部92に格納されている機器認証鍵KSを復号鍵として前記暗号アルゴリズムの復号部92において復号する。

【0077】 $X5 = D(KS, RES2)$

そしてその結果X5を第2のデータ分離部96に入力す

る。第2のデータ分離部96は入力されたデータX5を第2の乱数部分XX4と第3の乱数部分のデータKKに分離する。そして第2の乱数部分のデータXX4を第2のデータ比較部97に対して送出する。一方第2の乱数発生部94に一時記憶されている乱数R2は第2の暗号アルゴリズムの暗号器101に送られここで第6の認証鍵鍵格納部102に格納されている第2の機器認証鍵KS2を暗号鍵として暗号化される。

【0078】 $X_6 = e(KS_2, R_2)$

このデータX6は第2のデータ比較部97に送られ第2のデータ比較部97はこのデータを前記データXX4と比較する。これが一致すれば通信相手は正規の機器認証鍵を持っていることを証明したものと考え、通信相手が間違いない正規の機器であることを認証する。そして(6)に進む。もしも一致しなければ認証は失敗したものとして認証処理を終る。

(6) 第2のデータ分離部で分離された第3の乱数を第2の共有鍵一時格納部98に設定する。そして第1の機器70に対して認証した旨の信号を送る。

(7) 第2の機器90から認証した旨の信号を受けた第1の機器70は第3の乱数発生部77で生成した乱数Kを第1の共有鍵一時格納部79に転送する。そしてデータ暗号器80は著作物データ格納部81に格納されているデータをこの乱数Kを暗号鍵として用いて暗号化しその結果を通信路85に対して送出する。

(8) この電文を受け取った第2の機器90はデータ復号器99に入力されるデータを第2の共有鍵一時格納部98に格納されているデータを復号鍵として復号する。そしてこの結果を著作物処理部89において処理する。

【0079】もしも第1の機器が正規の認証鍵をすべてを有し、第2の機器が正規の認証鍵のうち有していないものがある場合、ステップ(3)で第1の機器は通信相手が正規の認証鍵を有していないものと判断し、認証処理が中断される。また第1の機器が正規の認証鍵のうちいずれかは有しておらず、第2の機器は正規の認証鍵をすべて有している場合、第2の機器は通信相手が正規の認証鍵を有していないものと判断し、認証処理を中断する。このようにして著作権データが不正な機器に流出することとともに不正な機器から正規の機器に流入することが防止できる。

【0080】この第2の実施例のポイントは、第1の実施例における暗号モジュールおよび復号モジュールとは異なる暗号変換および第2の認証鍵からなるモジュールを通信リンクに接続される両方の機器に備え、これを双方向認証プロトコルに併用したことにある。従って、第2の暗号器と第2の認証鍵を厳重に管理することにより、第1の実施例よりもさらに厳重な機器認証を行うことができる。

【0081】前記暗号モジュールと復号モジュールは通信リンクの両端に備わる通信制御のための集積回路に組

10

20

30

40

50

み込まれることにより効果的に実現することができる。一方、第2の暗号器と第2の認証鍵は前記暗号モジュールや復号モジュールよりもさらに厳重に管理されるべきであり、例えばシステムコントローラ用の集積回路に組み込まれることにより最も効果的に実現される。

【0082】なお、本実施例においては第2の暗号モジュールを第1および第2の機器に組み込み認証処理に関与させることについて説明したが、本発明はこの構成に限定されるものではなく、例えば第1の機器にはある暗号アルゴリズムの暗号モジュールを追加し、第2の機器にはこれに対応する復号モジュールを追加してこのモジュールにおける処理を双方向認証プロトコルに組み込むことも可能である。本発明の重要な点はこれらを厳重に管理することにより機器間通信保護装置の安全性をより高めることにある。

【0083】(実施例3) 次に、以上述べた機器間通信保護装置を例え、代表的な標準入出力インターフェースであるSCSI (Small Computer System Interfaceの略語) を用いたデータ伝送に適用した第3の実施例について説明する。本実施例は請求項5に対応するものである。

【0084】SCSIではある1対の機器は、バスを占有した後、コマンド、データ、ステータス、メッセージの4つのフェーズを遷移しながらデータを伝送する。例えば、第1の機器が第2の機器からデータを読み込む場合の典型的なフェーズ遷移は次のとおりである。

(1) コマンドフェーズ：第1の機器が第2の機器に対して、データ読み込みのコマンドを送出。

(2) データフェーズ：第2の機器から第1の機器に指定の長さのデータが送られる。

(3) ステータスフェーズ：第2の機器から第1の機器にコマンド実行結果の報告。

(4) メッセージフェーズ：第2の機器から第1の機器にコマンド終了メッセージ送出。

【0085】第3の実施例では、このコマンドに新たに認証と暗号鍵共有のコマンドと暗号通信コマンドを追加する。これらのコマンドを用いた第3の実施例の機器間通信保護装置の動作を、図5の第1の機器と第2の機器のやりとりを示す図に従い説明する。図5において120は第1の機器、121は第2の機器であり、その間のやりとりを上から順に示している。なお、図5では第1の機器が第2の機器からデータを読み込む場合について示す。

(1) コマンドフェーズ：第1の機器が第2の機器に対して、認証と暗号鍵共有のコマンドを送出する。

(2) データフェーズ：第1の機器と第2の機器の間で第2の実施例に従ったデータのやりとりを行なう。

【0086】(1)のコマンドに従い、第1の機器と第2の機器はチャレンジ・レスポンスのやりとりを行ない、片側または相互に通信相手の正当性を認証する。そし

て、この処理の結果として共通の暗号鍵を共有する。

(3) ステータスフェーズ：第2の機器から第1の機器に(1)のコマンド実行結果の報告。

(4) メッセージフェーズ：第2の機器から第1の機器に(1)のコマンド終了メッセージ送出。

(5) コマンドフェーズ：第1の機器が第2の機器に対して、暗号通信(読み込み)コマンドを送出する。

(6) データフェーズ：第2の機器から第1の機器に指定の長さのデータが送られる。

【0087】このとき、(5)のコマンドに従って、第2の機器は(2)で共有した共通の暗号鍵を用いてデータを暗号化して伝送する。第1の機器は伝送されたデータを受けとて、共通の暗号鍵で復号する。

(7) ステータスフェーズ：第2の機器から第1の機器に(5)のコマンド実行結果の報告。

(8) メッセージフェーズ：第2の機器から第1の機器に(5)のコマンド終了メッセージ送出。

【0088】なお、以上の説明ではSCSIをもとに説明を行なったが、何もそれに特定するわけではなく、上記のうちコマンドフェーズとデータフェーズを備える入出力インタフェーズであれば、そのコマンドに通信保護のためのコマンドを追加してデータフェーズで認証や暗号鍵の共有や暗号通信をすることにより実現できる。

【0089】また、SCSIではSCSIバスの有効利用のため、ディスコネクトとリコネクトの機能が備わっている。例えば大量のデータをディスクからの読み出すコマンドを実行する場合に、途中にシーク時間(ヘッド位置の移動のための時間)が入る場合がある。この間はデータの読みだしはできないので、バスが空いたままになってしまう。バスの使用効率を向上するため、こういった場合、一旦機器間のリンクを分断(ディスコネクト)して、他の機器に解放し、再びバスを使用する準備ができたら再度接続(リコネクト)を要求する。

【0090】第3の実施例でこのディスコネクトとリコネクト機能を備える場合には、ディスコネクトの前に相互の機器の間で、リコネクトの時に認証、暗号鍵共有、暗号通信を同いった手順で行なうのかを打ち合せる。このことは請求項6に関するものである。上記打ち合せる内容は例えば次のようなものである。

・リコネクトしたときに、上で述べた手順に従って再度通信相手の正当性の認証処理を行なうか。それとも簡易版として片側だけの認証を行なうのか。それとも行わないのか。

・リコネクトしたときに、上で述べた手順に従って再度共通の暗号鍵の設定を行なうか。それとも以前の暗号鍵を用いるか。この打合せを行なってからディスコネクトすることにより、リコネクトの際の双方のやりとりをスムーズに行なうことができる。

【0091】

10 【発明の効果】以上のように請求項1の発明は、認証プロトコルを実現するとき、一方の機器では暗号変換のみを行ない、他方の機器においては前記暗号変換の逆変換のみを行なうことが可能となり、暗号変換とその逆変換の両方を有する必要がなくコンパクトに実現できるようになった。

【0092】請求項2の発明は、認証および鍵共有プロトコルを実現するとき、一方の機器では暗号変換のみを行ない、他方の機器においては前記暗号変換の逆変換のみを行なうことが可能となり、暗号変換とその逆変換の両方を有する必要がなくコンパクトに実現できるようになった。

【0093】請求項3の発明は、暗号変換モジュールと暗号モジュール間、復号モジュールと復号モジュール間では認証ができないため、暗号モジュールまたは復号モジュールの一方の提供を厳重に管理することにより、装置間通信保護の効力を高めることができる。

20 20 【0094】請求項4の発明は前記暗号モジュールおよび復号モジュールとは異なる別のモジュールをより厳密な管理状態で提供することにより、装置間通信保護の効力を高めることができる。

【0095】請求項5および6の発明は、従来の機器間通信装置に正当性認証と暗号鍵共有と暗号伝送の保護機能のすべてまたはその一部の機能を追加したときに、上記の効果を発揮することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施例のブロック図

【図2】本発明の第1の実施例の動作説明図

【図3】本発明の第2の実施例のブロック図

【図4】本発明の第2の実施例の動作説明図

【図5】本発明の第3の実施例の動作説明図

【図6】従来の機器間通信保護装置の一例のブロック図

【図7】従来の機器間通信保護装置の一例の動作説明図

【図8】従来の機器間通信保護装置の他の例のブロック図

【図9】従来の機器間通信保護装置の他の例の動作説明図

【符号の説明】

7 1 第1の乱数発生器

7 2 暗号器

7 3 第1の認証鍵格納部

7 4 暗号モジュール

7 6 第1のデータ比較部

9 1 復号器

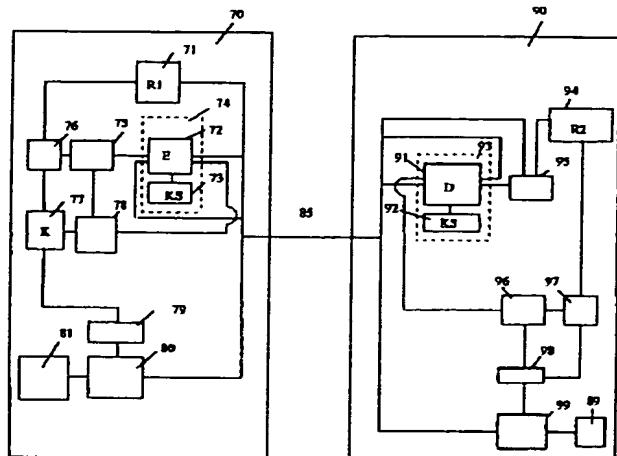
9 2 第2の認証鍵格納部

9 3 復号モジュール

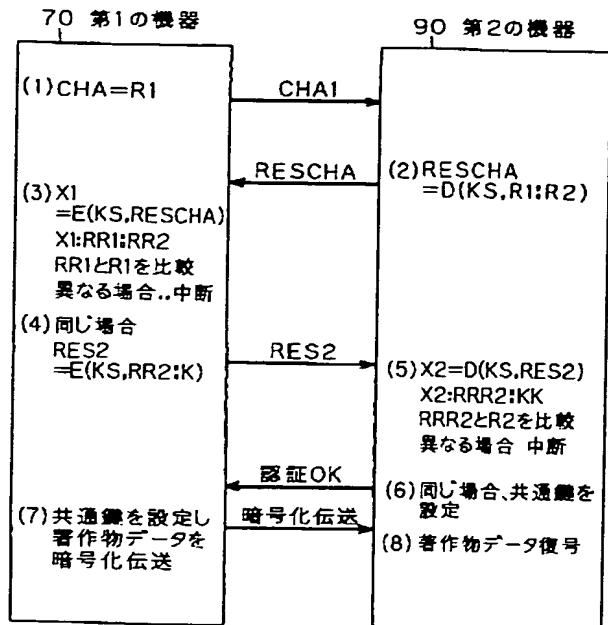
9 4 第2の乱数発生部

9 7 第2のデータ比較部

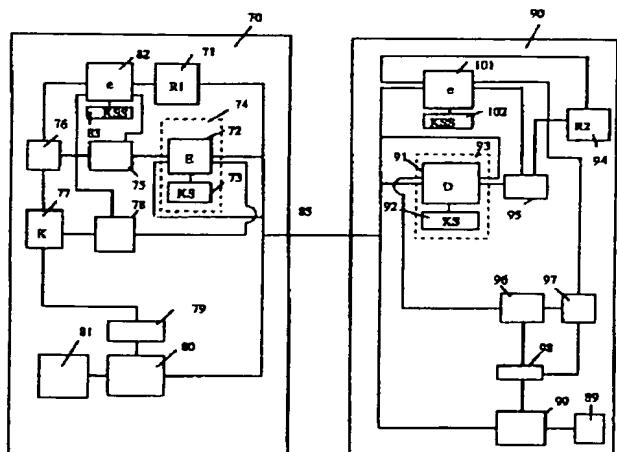
【図1】



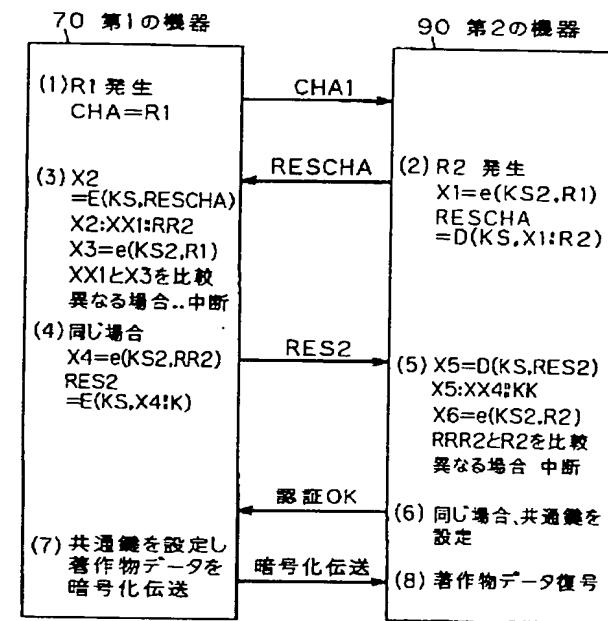
【図2】



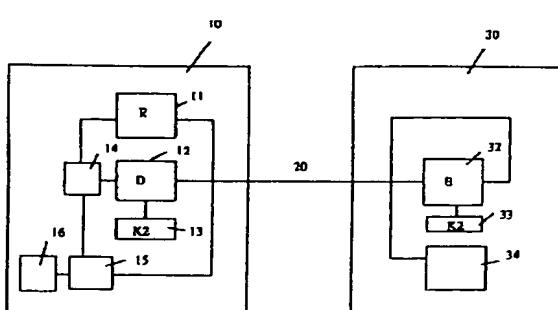
【図3】



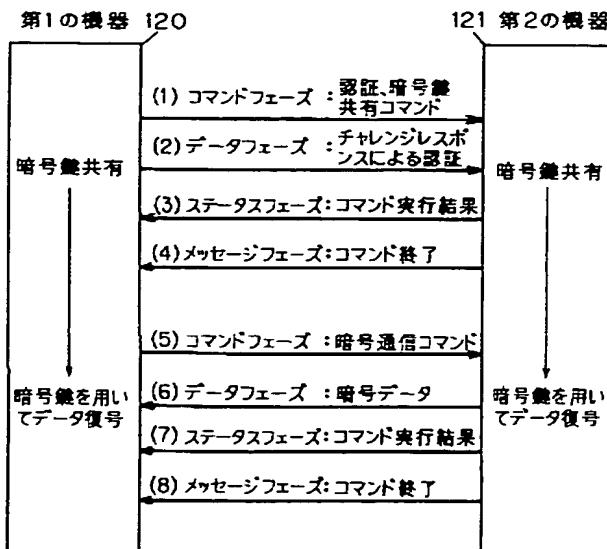
【図4】



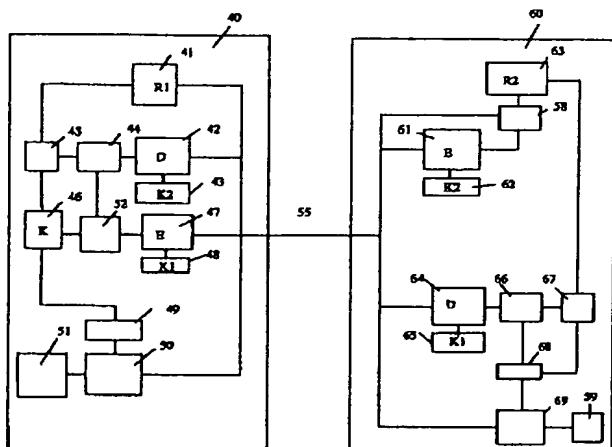
【図6】



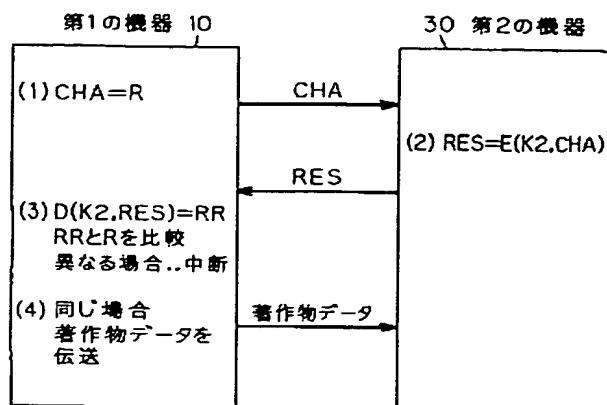
[図 5]



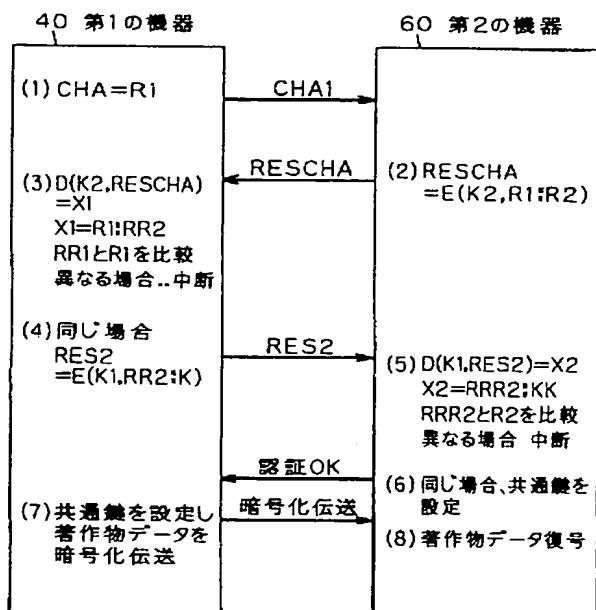
[図 8]



〔图7〕



[图 9]



フロントページの続き

(51) Int. Cl. ⁶

識別記号 庁内整理番号

E I

技術專示範所

H O 4 L 9/00

675 B

(72) 発明者 大森 基司

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 小塙 雅之

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 山内 一彦

大阪府門真市大字門真1006番地 松下電器
産業株式会社内